RANSOMWARE

Prevention & Response Guideline

(Draft Version 1.0)

BGD e-GOV CIRT

Table of Contents

Introduction

Ransomware attacks are deemed to be the most prevalent and damaging in today's cyber threat landscape. These attacks not only interrupt the victim's business operations, but also damage crucial data or files, rendering them unusable. This sort of cyber extortion may cost a business a lot of money, and the ransom isn't the only expense. Downtime, missed opportunities, ransomware removal, and recovery costs pile up quickly. Moreover, these attackers concentrate on encrypting backup data, further complicating the recovery procedure and rendering services inaccessible. In 2021, the average cost of a ransomware attack was $1.85 million, about double the previous year's expense [1].

TTP's (Tactics, Techniques, and Procedures) used by ransomware threat actors are becoming increasingly sophisticated. Threat actors that are "entrepreneurial" in nature are taking advantage of the expanding number of cybercriminals who want a piece of the ransomware pie. These criminal entrepreneurs provide ransomware as a service (RaaS) to other criminals, setting up agreements that specify the rules for distributing actual ransomware to these affiliates in exchange for a monthly fee or a percentage of the ransoms paid.

Multi-extortion techniques, in which an attacker encrypts an organization's files and also names and shames its victims and/or threatens to launch other attacks (e.g., distributed denial of service DDoS), are becoming more common. In 2021, 2,566 victims' names and proof of compromise were publicly released on ransomware leak sites, representing an 85 percent increase over 2020. These strategies are used by ransomware gangs to compel victims to pay more, faster, or both - albeit the

[1] https://www.cloudwards.net/ransomware-statistics/#Sources

effectiveness of the strategy is dependent in part on how important the data they've stolen is [2].

What is Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system or data and threatens to publish or sell data, until the victim pays a ransom fee to the attacker.

There are two main types of ransomwares:

- Encrypting files on the infected system are known as **crypto-ransomware.**
- Erase files or completely block access to the system using other methods, called **locker-ransomware.**

Ransomware uses a Public key to encrypt files and a Private key to unlock them, both of which can be created automatically in new combinations to infect new computers. Although file decryption methods may seem familiar, it is nearly impossible to decrypt without the Private key, and because each infected system generates new private keys, one victim's private key cannot be used to decrypt the data of another victim. The ransomware perpetrators hold these private keys on their servers, which they only share after the ransom is paid.

Objective of the guideline

This guideline is created to safeguard crucial and sensitive data from ransomware infection. This guideline will play a vital role to ensure secure usage, preservation and transfer of the Critical Information Infrastructures' (CII) data. Besides, it will also

[2] https://unit42.paloaltonetworks.com/2022-ransomware-threat-report-highlights/

provide necessary instructions for the data recovery procedure from the backup to ensure business continuity in the event of a disastrous situation in which systems are afflicted with ransomware. This guideline aims to ensure that all digital service providers in the country, as well as government entities that provide digital services to the nation have a seamless business operation, service provision, and functionality.

Ransomware Infection Vector

- Internet facing vulnerabilities and misconfiguration
- Phishing
- Unsecured remote desktop protocol connections
- Infection with a malware precursor
- Third party or Managed Service Provider (MSP)

Ransomware prevention checklist

Preventive measures for computer users

- Conduct security awareness training and educate computer users about ransomware attacks.
- End users, or computer users, should be given hands-on training on how to identify business critical data and when, why, and how to securely transfer it.
- Cyber attackers frequently utilize phishing email campaigns and/or social engineering techniques to gain initial access. These phishing emails usually contain document files or url links that may not appear suspicious at first glance, but a single click can infect someone's computer. This is why end users must be taught to spot phishing emails and questionable website links (URLs) in order to avoid clicking on them or reporting them to their company's cyber security team.

Preventive measures on software and network

- Unnecessary OS service and Network services should be stopped in order to prevent any possible exploitation
- Well known and renowned anti-malware/antivirus usage is highly recommended and should be updated regularly to prevent latest attacks.
- Regular update of the computer OS and installation of security patches
- To ensure better cyber security, computer networks should be 'SEGMENTED' (dividing a large computer network into a group of small networks) and business critical networks should be isolated in order to stop spreading of any problems from one network to another.
- Employ a strong email filtering system to block spam and phishing emails
- Strict policy and technical controls should be implemented so the computer users are restricted to run/install any unauthorized programs/software
- Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs.
- If not required then close the TCP port 3389 (RDP), 445 (SMB), 135 (Messenger Service), 139 (NetBios) to prevent any connection attempt. If access to these services is required then it should be confined in restricted networks.
- Microsoft office MACROS should be disabled. Usage of POWERSHELL could be restricted.
- Multi-factor authentication (MFA) could be enabled for the access to any technology portal
- Intrusion Detection System and Intrusion Prevention System (IDS and IPS) are highly recommended to prevent possible ransomware attacks.
- SIEM (security information and event management) systems should be used to collect logs from network devices, servers, and end user computers, which can subsequently be examined, as well as network traffic monitoring, to detect and minimize the risks of intrusion or malware infection.
- A full inventory of IT assets should be created for resource prioritization, and it can be used to assure that the right amount of computing resources are accessible for a ransomware attack response.

- Regular AUDIT of the IT infrastructures, Vulnerability Assessment and Penetration Testing (VA/PT) are advised to be done to find any cyber risks and weaknesses which can be mitigated with an immediate effect.

Preventive measures for third party or Managed Service Providers (MSPs)

- Cyber criminals may utilize third-party vendors or managed service providers (MSPs) to carry out ransomware attacks. If third-party vendors or managed service providers (MSPs) are hired to perform maintenance, they may be governed by an official agreement to follow 'Best Practices' in order to exchange sensitive data for the organization, which will aid in the prevention of cyber-attacks.
- Third-party vendors or managed service providers (MSPs) should be regulated so that they cannot impersonate or spoof the identity of an organization.
- Accounts, roles, and privileges used by MSPs for the associated organization's computer systems and network resources should be audited (at least every three months) to identify any risks and take the required steps to mitigate them.
- Shared accounts usage are not recommended
- If third-party vendors or managed service providers (MSPs) are required to provide services via ISPs (Internet Service Providers), only a verified Secure VPN Network should be used to access the organization's network, and access should be limited to only the time needed to provide the service or troubleshoot.
- Service recipients, third-party vendors, and managed service providers (MSPs) should all work together to anticipate any ransomware attack. In the event of such an attack, everyone's role should be clearly defined for proper incident response, a realistic plan for service restoration should be implemented, and a 'Tabletop Exercise' might be organized.

Backup based preventive measures

- Backups of business-critical data should be performed on a regular basis with considerable caution. Use the 3-2-1 backup strategy to back up your files. A 3-2-1 method suggests that you have at least three copies of your data, two of which are local but on separate mediums (read: devices), and one copy off-site/off-line.If data could not be recovered from the first two backups, the third backup, which is off-line/off-site, could be used instead.
- Regular data restoration should be performed from the backups to ensure data integrity.

Ransomware response checklist

Time-sensitive reactive measures:

- Immediately shutdown infected systems.
- Disconnect and isolate infected systems from the network.
- The ransomware-infected LAN (Local Area Network) may be disconnected and quarantined from the production network until it is fully recovered.
- If infected systems cannot be unplugged from the network, they should be shut down to prevent the infection from spreading throughout the whole network.
- Disable all shared drives that hold critical information.
- Use an organization-wide alert to notify about the attack.

Analysis-based reactive measures:

- Determine the scope and magnitude of an infection by identifying the type and number of devices infected, as well as what kind of data was encrypted.
- Once you've identified the type and version of ransomware, see if there's a decryption tool available online.

- Perform a root cause analysis to identify the threat vector that was used to infiltrate your network and take the required steps to mitigate any detected vulnerabilities to prevent future ransomware attacks.

Business continuity reactive measures:

- Progressively reconnect devices/subnets to the network and restore data from an unaffected offline backup, encrypted backups based on a prioritization of critical services.
- Once the environment has been cleaned and rebuilt (including affected accounts and the removal of malicious persistence mechanisms), mandate password resets for all accounts, and implement 2FA if possible.